For the Public Record

Wayland School Data Privacy: Committee Meeting Follow-up

21 January, 2016

To: **Wayland School Committee**
41 Cochituate Road
Wayland ,MA 01778

Dear members of the Wayland School Committee:

Thank you for the opportunity to present our additional concerns and updated letter at the School Committee meeting. It was interesting to hear the presentations from Dr. Stein and Leisha Simon. As Ellen Grieco requested, here are clarifications that should be helpful to Committee members:

Please: do not repeat four years of slow / no progress

Mark Hays has been trying to encourage WPS IT to upgrade security since 2012. In 2012, 2013, 2014 and 2015, Mark tried to prompt Wayland IT to take action. He identified important security upgrades WPS and Wayland needed, provided a guide to "next steps", made presentations to WPS IT staff, delivered samples of security standards and templates WPS could use, and volunteered to help WPS IT.

Unfortunately, Mark's recommendation in 2012 to install a patch management system was not implanted in 2012, 2013 or 2014 – and computers in the Wayland Treasurer's office were missing a two year old patch for Acrobat Reader.

The result? Hackers broke in and $4 million of Wayland taxpayer money almost vanished. Unibank happened to notice the transfer and called, "Do you really want to transfer $4 million to this account?" That's how close Wayland came to a massive theft.

In the School Committee meeting you heard many of the same things Mark heard in 2012, 2013, 2014 and 2015. You did not hear any commitments to deliver any upgrades on any date -- not even a date for a plan.

#1 recommendation: Require plans with clear dates and deliverables

Given this track record and the high cost of more delays, the School Committee needs to require Dr. Stein and WPS IT to (a) commit to dates to deliver plans for decisions and upgrades, and (b) deliver project plans with clear schedules and deliverables. Without firm commitments, expect more of the same.

Key security and IT management issues

1. Security updates missing from WPS computers

Focus on the plain fact: >1,700 WPS Macs were missing 2 or more major Apple security updates for 4 to 7 months. Although a number of explanations were offered by WPS IT, this long delay is not standard, "best practice" or acceptable. Every industry expert will agree.

It should be obvious: waiting for months "until a school break" to update computers is an invitation to disaster. No one with experience in IT security and management would think delays like this are necessary or reasonable.

- **"We had to install firmware updates manually."** This explanation for the delays was puzzling. Apple OS X updates commonly include a firmware update, which is part of the package and installs automatically. It would obviously be very time consuming if every school district and company that uses Apple products had to install these firmware updates by hand, computer after computer.
- **Mark Hays contacted JAMF, the vendor behind Casper**, to double-check. Here is their reply:

  > "Yes we can update machines with firmware updates. We can configure them with restart options and logic to ensure it's successful."

  Perhaps more training from JAMF would be helpful for the WPS IT team, to automate this process and improve WPS security. JAMF can provide custom training, and offers a number of standard courses online.

▶ As we recommended in our last letter, the School Committee should require WPS IT to use Casper to deliver updates quickly – *within days* of the release by Apple. You should also require monthly status reports from WPS IT that show the update status for all WPS computers. These reports are very easy to produce from Casper and WSUS. Oversight is required.

2. Casper is not a complete solution, even for Apple products

Everyone prefers the tools they are familiar with, and Casper has been with WPS for years. This software deployment product is only <u>half</u> of an endpoint security / patch management system, however. Here are four significant gaps:

- **When new patches are released, Casper does not automatically notify** IT staff, and does not automatically download the files for installation. Impact: There are many software products and vendors, and staff must constantly check for updates. One overlooked update can lead to a major vulnerability and data breach – like the Wayland Treasurer's Office, which was missing a patch for Acrobat Reader.

- **Casper does not automatically download and stage updates for "test"** or promote them for deployment when tests are complete. Impact: IT staff must find and download updates, manually shift them to a test environment, confirm test results, them manually move them into production. Casper does not provide automated patch workflow or logging, which means more wasted time. Critical patches may be overlooked or mis-routed during this repetitive manual process.
- **Casper does not automatically monitor Macs for missing patches**, and alert IT staff if a gap is found. Impact: A critical security patch may not have been installed due to a technical glitch or user intervention, creating a vulnerability which will go undetected – like the missing patch for Acrobat that led to the breach in the Wayland Treasurer's Office.
- **Casper cannot manage Windows or Chromebook systems**, which WPS will continue to use for years to come – despite the talk about a complete shift to Apple products. It is much more efficient to use one system to manage every endpoint.

If you read up on Casper and JAMF (the vendor), you will find that users have created dozens of work-arounds with custom "scripts" and functions, to try to automate patch workflow. This creates lots of extra work -- and job security for some. At the 2015 JAMF user conference, their CEO announced:

> "Quality first, Patch Management in the works but will be released when ready."

▶ Dr. Stein and the School Committee need to take action and get past this four-year delay. Both McCann and McGladrey recommended a new patch management system, and you should follow their advice.

3. No data encryption

We were told that WPS IT is "studying" encryption, but no time schedule or delivery commitments were offered – for a plan or implementation. Encryption is an industry, Commonwealth and Federal standard, particularly for portable computers that are easily lost or stolen – recommended by the US Department of Education. This is not an option based on opinion.

▶ The School Committee and Dr. Stein should take action and require a project plan and delivery date – with completion by 31 March, more than enough time for the any training that may be needed.

4. LanSchool monitoring of student computer use

We were puzzled by Ms. Simon's statement that there are "conflicting opinions about LanSchool" and she was going to "research" the issue. Mark Hays sent Ms. Simon information on LanSchool security problems in 2013 and again in April of 2015.

Mark notified Ms. Simon and the WPS IT team:

- Unauthorized people could access the LanSchool monitoring function.
- There was no log of "who monitored who when".
- Anyone with LanSchool access could monitor anybody.
- The user data logged by LanSchool was protected by very weak encryption, with a very simple hack widely available on the Web.

Mark’s son graduated from WHS last June and confirmed that students can block LanSchool monitoring, log on as ‘teachers’, view and control other students’ computers, play pranks on them, etc. Imagine the liability for WPS if someone misused LanSchool and recorded another student’s computer, chat sessions, credit card transactions, etc.

How is this possible? Anyone can download the LanSchool ‘Teacher’ app. Students can install it and spoof the system. For example, see:

- https://www.youtube.com/watch?v=4Bmn6xryYzU
- https://www.youtube.com/watch?v=AG-m_G6O5Qo

Mark Hays also contacted the vendor, Stoneware, to see if they are aware of the problem; Stoneware confirmed that this exploit is possible. The only suggestion they offered: use the LanSchool Security Monitor and ask an unfortunate employee to constantly watch for unauthorized users!

▶ Dr. Stein and the School Committee need to take immediate action and uninstall this system, to avoid abuse and misuse. Secure alternatives are available.

5. “Students cannot install software anyway”

This is also incorrect, as Mark’s son Zac can attest. WHS students know how to gain ‘Admin’ rights. Zac tried to show the WPS IT team how this could be done and demonstrated the process for them on his laptop, but the staff member simply said, “That’s impossible!”.

WPS “Admin” accounts were also easily hacked by WHS students, e.g. to login to the “Teacher” network. When another student brought this to WHS tech staff, he said “they didn’t care” and never followed up.

▶ First, Dr. Stein and the School Committee should ask Wayland IT to take a closer look at how they configure WPS computers and networks. A review by Zac Hays is attached with examples of specific problems. Second, Wayland IT should ensure that tech staff listen to student concerns and invite their input.

6. Google Apps for Education

We hope that you read the Electronic Frontier Foundation's request for an FTC injunction against Google. A Google spokeswoman also told *Education Week*,

> "… the company "scans and indexes" the emails of all Apps for Education users for a variety of purposes, including potential advertising, via automated processes that cannot be turned off—even for Apps for Education customers who elect not to receive ads."
>
> See: Education Week, March 26, 2014, "Google Under Fire for Data Analysis of Student Emails".

So how and why does Google mine our data, but *not send ads to students inside* Google Apps for Education (GAFE)? Simple: Google is a for-profit company, not a charity – and their main business is collecting and mining data across the Web. Even if Google doesn't deliver ads to Wayland students *inside* GAFE, they can mine our student data, create personal profiles for every student and deliver ads via Google Search and thousands of other websites.

Google's website tells a different story: "Google Apps for Education services don't collect or use student data for advertising purposes or create ads profiles." *See: https://support.google.com/a/answer/139019?hl=en*

Google's GAFE customer Agreement does not include these limits, however, and contradicts their marketing story. A copy of our analysis is attached for your review. We contacted Google directly, asking them to clarify the rights they claim under the GAFE customer agreement and a related amendment, and will keep you posted.

- ▶ Dr. Stein and the School Committee should prepare to budget for a replacement for 'free' GAFE applications. This is a good example of the need for a thorough review of each IT vendor, and a contract with each vendor that governs data privacy – as the US Department of Education recommends.

7. Outsource WPS computer management and security

- ▶ After everything you have learned over the past year, do you think Wayland and WPS computer systems have been managed well? Are you confident about computer security in Wayland Public Schools?

  Given what you now know, what does the School Committee intend to do? Will WPS hire a separate IT Director, or ask the new Town IT Director to manage WPS IT infrastructure too – including the much larger group of WPS computers? Or will WPS hire an outsourced computer services company? Or do you intend to continue down the same old path, despite McGladrey's recommendations?

8. **No insurance coverage for data breaches, tax dollars or people**

   ▶ Did you contact Nan Balmer to check the cost of additional insurance coverage to protect Wayland taxpayers, employees and Board / Committee members?

9. **Penetration testing:**

> " As a best practice, providers, schools, and districts may want to conduct periodic privacy audits to confirm that policies and procedures to ensure the security and confidentiality of the data are being followed."

McGladrey and our team recommended the same process for the Wayland network.

▶ Did you contact Nan Balmer to make sure the penetration testing that the Town plans to conduct will also cover WPS?

10. **A list of all Web and local software vendors used by WPS:**

    ▶ After the discovery of the problems with VoiceThread, it is clear that we need to review every IT vendor and product used by WPS, to make sure reliable and secure solutions have been selected. Please provide a list of all Web and locally installed software products and vendors used by WPS. We will be happy to assist with this review.

Please let us know if you have any questions. A number of us are happy to volunteer to help WPS evaluate IT vendors and solve these problems.

The Wayland Computer Privacy Initiative

CC: Wayland Board of Selectmen, Finance Committee, Dr. Paul Stein, Nan Balmer,
WTA and public media